UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/662,996	09/15/2003	Takashi Kawasaki	0828.68359	2241

24978   7590   01/16/2007
GREER, BURNS & CRAIN
300 S WACKER DR
25TH FLOOR
CHICAGO, IL 60606

EXAMINER
LUDWIG, PETER L

ART UNIT	PAPER NUMBER
3621	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

PTOL-90A (Rev. 10/06)

	Application No.	Applicant(s)
Office Action Summary	10/662,996	KAWASAKI ET AL.
	Examiner	Art Unit	
	Peter L. Ludwig	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 December 2003*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☒ All   b)☐ Some *   c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date *09/15/2003*.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2.   Claim 5 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant does not distinctly point out which decryption key is being used in line 13. There are two decryption keys pointed out and examiner is unsure if they are the same or different and how they are obtained.

3.   Claim 13 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant does not distinctly point out how the determination is being performed in lines 18-20. There are many ways to perform this determination, which are all different.

Claim Rejections - 35 USC § 102

4.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in The United States.

5.   Claims 1-12, and 14-20 are rejected under 35 U.S.C. 102(b) as being anticipated by

Downs et al. (U.S. Patent No. 6,226,618) [hereinafter Downs].

6.   As per claim 1, Downs teaches a license issuance server for issuing a license for

execution of software, comprising:

- **software encryption key generating means** (Step Process 301 Sender generates a

   random symmetric key and uses it to encrypt the content. 302 Sender runs the encrypted

   content through a hash algorithm to produce the content digest (Fig. 3, col. 15)),

   responsive to an encryption key generation request for the software (When the End-

   User(s) completes shopping they submit the purchase request to the Electronic digital

   Content Store(s) 103 for processing (col. 18)), **for generating a software encryption**

   key and a software decryption key for decrypting the software encrypted using the

   software encryption key (Fig. 1D);

- **license issuing means, responsive to a license issue request including device**

   identification information fixedly recorded on a recording medium in a processing

   device which is a target of permission to run the software (The Clearinghouse

   Transaction Log 178 can be used by the Content Provider(s) 101 to determine what

   Content 113 of his has been sold and enables him to create a bill to each Electronic

Digital Content Store(s) 103 for royalties owed him. Other electronic means besides

billing can alternatively be used to settle accounts between the Content Provider(s) 101

and Electronic Digital Content Store(s) 103 (Fig. 9, col. 76, lines 18-25)), **for encrypting**

the software decryption key by using the device identification information and

outputting a software license including the encrypted software decryption key (The

data is encrypted so as to only be decryptable by a data decrypting key, the data

decrypting key being encrypted using a first public key, and the encrypted data being

accessible to the user's system (abstract); both the Content 113 and the Keys (described

below) are encrypted and packed in SCs, Electronic Digital Content Store(s) 103 or any

other hosting agent can not directly access decrypted Content 113 without clearance from

the Clearinghouse(s) and notification to the Content Provider(s) 101(col. 9, lines 55-60)).

7.   As per claim 2, Downs teaches claim 1 as described above. Downs further teaches

wherein, if the encryption key generation request is received from a different computer

connected via a network, said software encryption key generating means transmits the

generated software encryption key to said different computer (The Secure Digital Content

Electronic Distribution System 100 is independent of the transmission network connecting the

Electronic Digital Content Store(s) 103 and End-User Device(s) 109. It supports both point-to-

point such as the Internet and broadcast distribution models such as broadcast television (col. 11,

lines 56-61)).

8.   As per claim 3, Downs teaches claim 1 as described above. Downs further teaches

wherein, if the license issue request is received from a different computer connected via a

network, said license issuing means transmits the generated software license to said

different computer (Only users who have decryption keys can unlock the encrypted Content,
and the Clearinghouse(s) releases decryption keys only for authorized and appropriate usage
requests. The Clearinghouse(s) will not clear bogus requests from unknown or unauthorized
parties or requests that do not comply with the content's usage conditions as set by the content
proprietors (col. 7, lines 31-37; Examiner is interpreting this as the ability to facilitate with
"different" computers)).

9.   As per claim 4, Downs teaches a software provision server for providing software whose
execution is to be restricted by a license, comprising:

- **software encryption key generating means, responsive to an encryption key
  generation request for the software, for generating a software encryption key and a
  software decryption key for decrypting the software encrypted using the software
  encryption key** (The data is encrypted so as to only be decryptable by a data decrypting
  key, the data decrypting key being encrypted using a first public key, and the encrypted
  data being accessible to the user's system (col. 3, lines 42-46), If the requested use of the
  content does not comply with the usage conditions, e.g., the number of copies has been
  exhausted, the End-User Device(s) will not perform the request (col. 7, lines 52-55));

- **software encrypting means for encrypting the software by using the software
  encryption key generated by said software encryption key generating means** (Step
  Process 301 Sender generates a random symmetric key and uses it to encrypt the content
  (Fig. 3, col. 15));

- **software providing means, responsive to input of a software request which is received from a processing device as a target of permission to run the software (Fig. 1B) and which includes device identification information fixedly recorded on a recording medium in the processing device, for transmitting the software encrypted by said software encrypting means to the processing device** (A second watermark is embedded in the Content at the End-User Device(s) to identify the content purchaser (or licensee) and End-User Device(s), specify the purchase or license conditions and date, and add any other pertinent information (col. 7, lines 61-65); The End-User Device(s) 109 can be any player device that contains an End-User Player Application 195 (described later) compliant with the Secure Digital Content Electronic Distribution System 100 specifications. These devices may include PCS, set top boxes (IRDs), and Internet appliances. The End-User Player Application 195 could be implemented in software and/or consumer electronics hardware. In addition to performing play, record, and library management functions, the End-User Player Application 195 performs SC processing to enable rights management in the End-User Device(s) 109. The End-User Device(s) 109 manages the download and storage of the SCs containing the Digital Content; requests and manages receipt of the encrypted Digital Content keys from the Clearinghouse(s) 105; processes the watermark(s) every time the Digital Content is copied or played; manages the number of copies made (or deletion of the copy) in accordance with the Digital Content's Usage Conditions; and performs the copy to an external media or portable consumer device if permitted. The portable consumer device can perform a subset of the End-User Player Application 195 functions in order to

process the content's Usage Conditions embedded in the watermark (col. 11, lines 30-

52));

- **license issuing means** (End-User(s) that have secured a license (col. 7, lines 4-5),

  responsive to input of the software request from the processing device, for

  encrypting the software decryption key by using the device identification

  information and outputting a software license including the encrypted software

  decryption key to the processing device (After inscribing any required watermark to

  this content buffer, the buffer is passed to the scrambling function for Re-Encryption 194.

  A processor efficient secure encryption algorithm such as IBM's SEAL encryption

  technology is used to re-encrypt the Content 113 using a random Symmetric Key (Fig.

  1D; col. 82, lines 28-34; Examiner is interpreting the watermark to hold the identification

  information as stated earlier)).

10.   As per claim 5, Downs further teaches a processing device for executing software whose

execution is restricted by a license, comprising:

- **a recording medium on which device identification information is fixedly recorded**

  (Since watermarks become an integral part of the Content, they are carried in the copies

  independent of whether the copies were authorized or not. Thus the Digital Content

  always contains information regarding its source and its permitted use regardless of

  where the content resides or where it comes from. This information may be used to

  combat illegal use of the Content (col. 7-8, lines 66-67 and 1-5));

- **decryption key decrypting means, responsive to reception of a software decryption key which has been encrypted, for decrypting the software decryption key by using the device identification information recorded on said recording medium as a decryption key** (The Clearinghouse(s) 105 provides the licensing authorization and record keeping for all transactions that relate to the sale and/or permitted use of the Content 113 encrypted in a SC. When the Clearinghouse(s) 105 receives a request for a decryption key for the Content 113 from an intermediate or End-User(s), the Clearinghouse(s) 105 validates the integrity and authenticity of the information in the request; verifies that the request was authorized by an Electronic Digital Content Store(s) or Content Provider(s) 101; **and verifies that the requested usage complies with the content Usage Conditions** as defined by the Content Provider(s) 101. Once these verifications are satisfied, the Clearinghouse(s) 105 sends the decryption key for the Content 113 to the requesting End-User(s) packed in a License SC. The key is encrypted in a manner so that only the **authorized user** can retrieve it. If the End-User's request is not verifiable, complete, or authorized, the Clearinghouse(s) 105 repudiates the request for the decryption key (col. 10, lines 50-72));

- **software decrypting means, responsive to reception from a software provision server of the software which has been encrypted, for decrypting the software by using the software decryption key decrypted by said decryption key decrypting means as a decryption key** (The Clearinghouse(s) 105 provides the licensing authorization and record keeping for all transactions that relate to the sale and/or permitted use of the Content 113 encrypted in a SC. When the Clearinghouse(s) 105

receives a request for a decryption key for the Content 113 from an intermediate or End-User(s), the Clearinghouse(s) 105 validates the integrity and authenticity of the information in the request; verifies that the request was authorized by an Electronic Digital Content Store(s) or Content Provider(s) 101; **and verifies that the requested usage complies with the content Usage Conditions** as defined by the Content Provider(s) 101. Once these verifications are satisfied, the Clearinghouse(s) 105 sends the decryption key for the Content 113 to the requesting End-User(s) packed in a License SC. The key is encrypted in a manner so that only the **authorized user** can retrieve it. If the End-User's request is not verifiable, complete, or authorized, the Clearinghouse(s) 105 repudiates the request for the decryption key (col. 10, lines 50-72; Examiner is interpreting the fact that the encrypted package containing the decrypting key is only available to the 'authorized user' that this is a decryption key for the encrypted package)).

11.   As per claim 6, Downs teaches a license issuance server for issuing a license for execution of software, comprising:

- **attach/detach key information issuing means, responsive to an attach/detach key information generation request including device identification information fixedly recorded on a recording medium in a processing device which is a target of permission to run the software, for generating attach/detach key information including the device identification information and an attach/detach key-specific encryption key (Fig. 1A), and recording the generated attach/detach key information on a hardware key which can be attached to and detached from the processing device** (It should be understood that this process like any of the other

processes described on the Work Flow Manager 154 can run on a variety of hardware and

software platforms. This method may be practiced on any computer readable medium,

including but not limited to floppy diskettes, CD ROMS and removable hard disk drives

(col. 53-54 and lines 65-67 and 1-3), A Work Flow Manager Tool 154 schedules Content

113 to be processed and tracks the Content 113 as it flows through the various steps of

Content 113 preparation and packaging to maintain high quality assurance (col. 9, lines

18-21). These can be adapted to follow technical advances in digital content

compression/encoding, encryption, and formatting methods, allowing the Content

Provider(s) 101 to utilize best tools as they evolve over time in the marketplace (col. 9,

lines 43-47));

- · **license issuing means, responsive to a license issue request for the software, for

  encrypting a software decryption key for decrypting the software which is provided

  in an encrypted state** (The data is encrypted so as to only be decryptable by a data

  decrypting key, the data decrypting key being encrypted using a first public key,

  (abstract)), **by using the attach/detach key-specific encryption key, and outputting

  license information including the encrypted software decryption key** (and the

  encrypted data being accessible to the user's system (abstract; Examiner is interpreting

  the fact that the attach/detach mechanism can be used for the invention that any

  encryption key assigned to the device is specific to that device)).

12.   As per claim 7, Downs teaches claim 6 as described above. Downs further teaches

**wherein said license issuing means includes, in the license information, a license count

indicating a number of devices permitted to simultaneously execute the software** (Usage

Conditions – A part that contains information that describes usage options, rules, and restrictions to be imposed on an End-User (s) for use of the Content (col. 29, lines 40-42)).

13.   As per claim 8, Downs teaches claim 6 as described above. Downs further teaches **wherein said hardware key has tamper resistance** (The Secret User Key (not shown) is protected by breaking the key into multiple parts and storing pieces of the key in multiple locations throughout the End-User(s)' computer. This area of the code is protected with Tamper Resistant Software technology so as not to divulge how the key is segmented and where it is stored. Preventing access to this key by even the End-User(s) helps to prevent piracy or sharing of the Content 113 with other computers (col. 80, lines 30-38)).

14.   As per claim 9, Downs teaches claim 6 as described above. Downs further teaches **wherein said license issuing means encrypts the license information before outputting same** (Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract)).

15.   As per claim 10, Downs teaches claim 9 as described above. Downs further teaches **wherein said license issuing means encrypts the license information by using the attach/detach key-specific encryption key** (Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract)).

16.   As per claim 11, Downs teaches claim 6 as described above. Downs further teaches

further comprising license issue charge calculating means for storing past records on the

license information output from said license issuing means, and calculating, based on the

stored license information, a license issue charge to be billed to a provider of the software

(The Clearinghouse Transaction Log 178 can be used by the Content Provider(s) 101 to

determine what Content 113 of his has been sold and enables him to create a bill to each

Electronic Digital Content Store(s) 103 for royalties owed him. Other electronic means besides

billing can alternatively be used to settle accounts between the Content Provider(s) 101 and

Electronic Digital Content Store(s) 103 (col. 76, lines 18-25)).

17.   As per claim 12, Downs teaches a software provision server for providing software

whose execution is to be restricted by a license, comprising:

- **attach/detach key information issuing means, responsive to an attach/detach key**

  information generation request including device identification information fixedly

  recorded on a recording medium in a processing device which is a target of

  permission to run the software, for generating attach/detach key information

  including the device identification information and an attach/detach key-specific

  encryption key (Fig. 1A), and recording the generated attach/detach key

  information on a hardware key which can be attached to and detached from the

  processing device (It should be understood that this process like any of the other

  processes described on the Work Flow Manager 154 can run on a variety of hardware and

  software platforms. This method may be practiced on any computer readable medium,

  including but not limited to floppy diskettes, CD ROMS and removable hard disk drives

(col. 53-54 and lines 65-67 and 1-3), A Work Flow Manager Tool 154 schedules Content 113 to be processed and tracks the Content 113 as it flows through the various steps of Content 113 preparation and packaging to maintain high quality assurance (col. 9, lines 18-21). These can be adapted to follow technical advances in digital content compression/encoding, encryption, and formatting methods, allowing the Content Provider(s) 101 to utilize best tools as they evolve over time in the marketplace (col. 9, lines 43-47));

- **software encryption key generating means** (Step Process 301 Sender generates a random symmetric key and uses it to encrypt the content. 302 Sender runs the encrypted content through a hash algorithm to produce the content digest (Fig. 3, col. 15)) **for generating a software encryption key for encrypting and decrypting the software, and a software decryption key for decrypting data encrypted by using the software encryption key** (The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract));

- **software encrypting means for encrypting the software by using the software encryption key generated by said software encryption key generating means** (The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract));

- **software providing means, responsive to input of a software request from the processing device, for transmitting the software encrypted by said software encrypting means to the processing device** (The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract));

- **license issuing means, responsive to a license issue request for the software, for encrypting the software decryption key by using the attach/detach key-specific encryption key, and outputting license information including the encrypted software decryption key** (The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key... and the encrypted data being accessible to the user's system (abstract; Examiner is interpreting the fact that the attach/detach mechanism can be used for the invention that any encryption key assigned to said device is specific to said device)).

18.   As per claim 14, Downs teaches a software execution management device for managing status of execution of software whose execution is restricted by a license, comprising:

- **a recording medium on which device identification information is fixedly recorded** (Since watermarks become an integral part of the Content, they are carried in the copies independent of whether the copies were authorized or not. Thus the Digital Content always contains information regarding its source and its permitted use regardless of where the content resides or where it comes from. This information may be used to combat illegal use of the Content (col. 7-8, lines 66-67 and 1-5));

- **hardware key connecting means for reading attach/detach key information including an attach/detach key-specific encryption key and permission target device identification information specifying a device which is a target of permission to run the software, from a hardware key storing the attach/detach key information when the hardware key is attached** (It should be understood that this process like any of the other processes described on the Work Flow Manager 154 can run on a variety of hardware and software platforms. This method may be practiced on any computer readable medium, including but not limited to floppy diskettes, CD ROMS and removable hard disk drives (col. 53-54 and lines 65-67 and 1-3); A Work Flow Manager Tool 154 schedules Content 113 to be processed and tracks the Content 113 as it flows through the various steps of Content 113 preparation and packaging to maintain high quality assurance (col. 9, lines 18-21). These can be adapted to follow technical advances in digital content compression/encoding, encryption, and formatting methods, allowing the Content Provider(s) 101 to utilize best tools as they evolve over time in the marketplace (col. 9, lines 43-47), Another encrypted object, in this example a Transaction ID encrypted object 205 is shown. And Usage Conditions 206 for content licensing management as described below. The SC(s) 200 comprises Usage Conditions 206, Transaction ID encrypted object 205, an Application ID encrypted object 207, and encrypted symmetric key object 204, all signed with an End-User Digital Signature 202 (col. 14-15, lines 63-67 and 1-5));

- **software key decrypting means, responsive to input of license information including an encrypted software decryption key for decrypting the software which has been**

encrypted and a number of computers permitted to execute the software simultaneously, for decrypting the software decryption key by using the attach/detach key-specific encryption key (It should be understood that this process like any of the other processes described on the Work Flow Manager 154 can run on a variety of hardware and software platforms. This method may be practiced on any computer readable medium, including but not limited to floppy diskettes, CD ROMS and removable hard disk drives (col. 53-54 and lines 65-67 and 1-3); Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract; Examiner is interpreting "a number of computers" as allowing one computer connected));

- **decryption key managing means for monitoring computers connected via a network to detect a number of computers executing the software, and transferring the software decryption key decrypted by said software key decrypting means to a number of computers equal to or smaller than the number of computers permitted to execute the software simultaneously** (Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract); The Content Dispersement Tool provides a user the ability to implement the Content Dispersement Process 814 as described above. Once the Content 113 has been approved

for release, the SC(s) for the Content 113 are placed in the queue of the Content

Dispersement Process. The Content Dispersement Tool monitors the queue and performs

immediate transfer of the SC(s) files or batch transfer of a group of SC(s) files based on

the configuration settings provided by the Content Provider(s) 101. The Content

Provider(s) 101 can also optionally configure the Content Dispersement Tool to

automatically hold all SC(s) in this queue until they are manually flagged for release (col.

67, lines 35-46)).

19.   As per claim 15, Downs teaches a license issuing method for issuing a license for

execution of software, comprising the steps of:

- **generating, in response to an encryption key generation request for the software, a**
  software encryption key and a software decryption key for decrypting the software
  encrypted by using the software encryption key (When the End- User(s) completes

  shopping they submit the purchase request to the Electronic digital Content Store(s) 103

  for processing (col. 18); Disclosed is a method and apparatus of securely providing data

  to a user's system. The data is encrypted so as to only be decryptable by a data decrypting

  key, the data decrypting key being encrypted using a first public key, and the encrypted

  data being accessible to the user's system (abstract));

- **encrypting, in response to a license issue request including device identification**
  information fixedly recorded on a recording medium in a processing device which is
  a target of permission to run the software, the software decryption key by using the
  device identification information, and outputting a software license including the

encrypted software decryption key (Disclosed is a method and apparatus of securely

providing data to a user's system. The data is encrypted so as to only be decryptable by a

data decrypting key, the data decrypting key being encrypted using a first public key, and

the encrypted data being accessible to the user's system (abstract) A second watermark is

embedded in the Content at the End-User Device(s) to identify the content purchaser (or

licensee) and End-User Device(s), specify the purchase or license conditions and date,

and add any other pertinent information (col. 7, lines 61-65); The End-User Device(s)

109 can be any player device that contains an End-User Player Application 195

(described later) compliant with the Secure Digital Content Electronic Distribution

System 100 specifications. These devices may include PCS, set top boxes (IRDs), and

Internet appliances (col. 11, lines 30-34)).

16.   As per claim 16, Downs teaches a license issuing method for issuing a license for

execution of software, comprising the steps of:

- **generating, in response to an attach/detach key information generation request**
  including device identification information fixedly recorded on a recording medium
  in a processing device which is a target of permission to run the software,
  attach/detach key information including the device identification information and
  an attach/detach key-specific encryption key, and recording the generated
  attach/detach key information on a hardware key which can be attached to and
  detached from the processing device (It should be understood that this process like any

  of the other processes described on the Work Flow Manager 154 can run on a variety of

  hardware and software platforms. This method may be practiced on any computer

readable medium, including but not limited to floppy diskettes, CD ROMS and

removable hard disk drives (col. 53-54 and lines 65-67 and 1-3); Fig. 5, The Content 113

is stored in the End-User Device(s) 109 in compressed form to reduce the storage size

requirement (col. 27, lines 15-17));

- **encrypting, in response to a license issue request for the software, a software
  decryption key for decrypting the software provided in an encrypted state, by using
  the attach/detach key-specific encryption key, and outputting license information
  including the encrypted software decryption key** (When the End- User(s) completes

  shopping they submit the purchase request to the Electronic digital Content Store(s) 103

  for processing (col. 18); Disclosed is a method and apparatus of securely providing data

  to a user's system. The data is encrypted so as to only be decryptable by a data decrypting

  key, the data decrypting key being encrypted using a first public key, and the encrypted

  data being accessible to the user's system (abstract)).

17.   As per claim 17, Downs teaches a license issuing program for issuing a license for

execution of software, wherein said license issuing program causes a computer to perform the

processes of:

- **generating, in response to an encryption key generation request for the software, a
  software encryption key and a software decryption key for decrypting the software
  encrypted by using the software encryption key** (When the End- User(s) completes

  shopping they submit the purchase request to the Electronic digital Content Store(s) 103

  for processing (col. 18); Disclosed is a method and apparatus of securely providing data

to a user's system. The data is encrypted so as to only be decryptable by a data decrypting

key, the data decrypting key being encrypted using a first public key, and the encrypted

data being accessible to the user's system (abstract));

■ **encrypting, in response to a license issue request including device identification**

information fixedly recorded on a recording medium in a processing device which is

a target of permission to run the software, the software decryption key by using the

device identification information, and outputting a software license including the

encrypted software decryption key (Disclosed is a method and apparatus of securely

providing data to a user's system. The data is encrypted so as to only be decryptable by a

data decrypting key, the data decrypting key being encrypted using a first public key, and

the encrypted data being accessible to the user's system (abstract) A second watermark is

embedded in the Content at the End-User Device(s) to identify the content purchaser (or

licensee) and End-User Device(s), specify the purchase or license conditions and date,

and add any other pertinent information (col. 7, lines 61-65); The End-User Device(s)

109 can be any player device that contains an End-User Player Application 195

(described later) compliant with the Secure Digital Content Electronic Distribution

System 100 specifications. These devices may include PCS, set top boxes (IRDs), and

Internet appliances (col. 11, lines 30-34)).

18.   As per claim 18, Downs teaches a license issuing program for issuing a license for

execution of software, wherein said license issuing program causes a computer to perform the

processes of:

- **generating, in response to an attach/detach key information generation request including device identification information fixedly recorded on a recording medium in a processing device which is a target of permission to run the software, attach/detach key information including the device identification information and an attach/detach key-specific encryption key, and recording the generated attach/detach key information on a hardware key which can be attached to and detached from the processing device** (It should be understood that this process like any of the other processes described on the Work Flow Manager 154 can run on a variety of hardware and software platforms. This method may be practiced on any computer readable medium, including but not limited to floppy diskettes, CD ROMS and removable hard disk drives (col. 53-54 and lines 65-67 and 1-3); Fig. 5, The Content 113 is stored in the End-User Device(s) 109 in compressed form to reduce the storage size requirement (col. 27, lines 15-17));

- **encrypting, in response to a license issue request for the software, a software decryption key for decrypting the software provided in an encrypted state, by using the attach/detach key-specific encryption key, and outputting license information including the encrypted software decryption key** (When the End- User(s) completes shopping they submit the purchase request to the Electronic digital Content Store(s) 103 for processing (col. 18); Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract)).

19.   As per claim 19, Downs teaches a computer-readable recording medium recording a

license issuing program for issuing a license for execution of software, wherein the license

issuing program causes the computer to perform the processes of:

- **generating, in response to an encryption key generation request for the software, a**
  software encryption key and a software decryption key for decrypting the software
  encrypted by using the software encryption key (When the End- User(s) completes

  shopping they submit the purchase request to the Electronic digital Content Store(s) 103

  for processing (col. 18); Disclosed is a method and apparatus of securely providing data

  to a user's system. The data is encrypted so as to only be decryptable by a data decrypting

  key, the data decrypting key being encrypted using a first public key, and the encrypted

  data being accessible to the user's system (abstract));

- **encrypting, in response to a license issue request including device identification**
  information fixedly recorded on a recording medium in a processing device which is
  a target of permission to run the software, the software decryption key by using the
  device identification information, and outputting a software license including the
  encrypted software decryption key (Disclosed is a method and apparatus of securely

  providing data to a user's system. The data is encrypted so as to only be decryptable by a

  data decrypting key, the data decrypting key being encrypted using a first public key, and

  the encrypted data being accessible to the user's system (abstract) A second watermark is

  embedded in the Content at the End-User Device(s) to identify the content purchaser (or

  licensee) and End-User Device(s), specify the purchase or license conditions and date,

  and add any other pertinent information (col. 7, lines 61-65); The End-User Device(s)

109 can be any player device that contains an End-User Player Application 195 (described later) compliant with the Secure Digital Content Electronic Distribution System 100 specifications. These devices may include PCS, set top boxes (IRDs), and Internet appliances (col. 11, lines 30-34)).

20.   As per claim 20, Downs teaches a computer-readable recording medium recording a license issuing program for issuing a license for execution of software, wherein the license issuing program causes the computer to perform the processes of:

- **generating, in response to an attach/detach key information generation request including device identification information fixedly recorded on a recording medium in a processing device which is a target of permission to run the software, attach/detach key information including the device identification information and an attach/detach key-specific encryption key, and recording the generated attach/detach key information on a hardware key which can be attached to and detached from the processing device** (It should be understood that this process like any of the other processes described on the Work Flow Manager 154 can run on a variety of hardware and software platforms. This method may be practiced on any computer readable medium, including but not limited to floppy diskettes, CD ROMS and removable hard disk drives (col. 53-54 and lines 65-67 and 1-3); Fig. 5, The Content 113 is stored in the End-User Device(s) 109 in compressed form to reduce the storage size requirement (col. 27, lines 15-17));

- **encrypting, in response to a license issue request for the software, a software decryption key for decrypting the software provided in an encrypted state, by using the attach/detach key-specific encryption key, and outputting license information including the encrypted software decryption key** (When the End- User(s) completes shopping they submit the purchase request to the Electronic digital Content Store(s) 103 for processing (col. 18); Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract)).

Claim Rejections - 35 USC § 103

20.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

21.   Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Downs in view of

Johnson et al. (U.S. Patent No. 5,859,935).

22.   As per claim 13, Downs teaches a processing device for executing software whose

execution is restricted by a license, comprising:

- **a recording medium on which device identification information is fixedly recorded**
  (Since watermarks become an integral part of the Content, they are carried in the copies
  independent of whether the copies were authorized or not. Thus the Digital Content
  always contains information regarding its source and its permitted use regardless of
  where the content resides or where it comes from. This information may be used to
  combat illegal use of the Content (col. 7-8, lines 66-67 and 1-5));

- **hardware key connecting means for reading attach/detach key information** (It
  should be understood that this process like any of the other processes described on the
  Work Flow Manager 154 can run on a variety of hardware and software platforms. This
  method may be practiced on any computer readable medium, including but not limited to
  floppy diskettes, CD ROMS and removable hard disk drives (col. 53-54 and lines 65-67
  and 1-3)) **including an attach/detach key-specific encryption key and permission**

target device identification information specifying a device which is a target of permission to run the software, from a hardware key storing the attach/detach key information when the hardware key is attached (A Work Flow Manager Tool 154 schedules Content 113 to be processed and tracks the Content 113 as it flows through the various steps of Content 113 preparation and packaging to maintain high quality assurance (col. 9, lines 18-21). These can be adapted to follow technical advances in digital content compression/encoding, encryption, and formatting methods, allowing the Content Provider(s) 101 to utilize best tools as they evolve over time in the marketplace (col. 9, lines 43-47));

■ **software key decrypting means, responsive to input of license information including an encrypted software decryption key for decrypting the software which has been encrypted, for decrypting the software decryption key by using the attach/detach key-specific encryption key** (Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract));

■ **identification information determining means for determining sameness of the permission target device identification information included in the hardware key attached to said hardware key connecting means with the device identification information recorded on said recording medium** (It should be understood that this process like any of the other processes described on the Work Flow Manager 154 can run on a variety of hardware and software platforms. This method may be practiced on any

computer readable medium, including but not limited to floppy diskettes, CD ROMS and

removable hard disk drives (col. 53-54 and lines 65-67 and 1-3); Fig. 2, The SC(s) 200

comprises Usage Conditions 206, Transaction ID encrypted object 205, an Application

ID encrypted object 207, and encrypted symmetric key object 204, all signed with an

End-User Digital Signature 202 (col. 15, lines 1-5));

- **software decrypting means for decrypting the encrypted software by using the software decryption key decrypted by said software key decrypting means if the sameness is confirmed by said identification information determining means** (Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract)).

However, Downs does not further teach the determination of sameness briefly described in the claim. Also, Downs does not teach wherein if the determination does come out equivalent, then the software gets sent to the issuer.

Johnson does teach the determination of sameness (Original source verifying data defining a first source verifying image are stored in memory. The first source verifying image can be produced by a human making marks by hand in a field of a form, which can then be provided by a scanner or a facsimile transmission through image input circuitry. If a second source verifying image is received that is the same as the first source verifying image, an operation is performed that

would not be performed if the images were not the same, such as an operation accessing a related

item of data (abstract); A "sameness criterion" is a criterion that can be applied to an item of data

indicating a measure of similarity between two images to obtain an item of data indicating

whether the two images are the same (col. 8, lines 5-12)).

Johnson also teaches wherein this verification of sameness must be performed before the action

of transferring data can take place (For example, the first source verifying image can be received

with a document image, and data defining the document image and the original source verifying

data can be stored so that a source verifying image that is the same as the first source verifying

image must be received before an operation can access the document data and provide it to

image output circuitry for printing or facsimile transmission (abstract)).

Therefore, it would have been prima facie obvious to one of ordinary skill in the art at the time of

the invention to incorporate the determination of sameness with Downs, for the useful purpose of

indicating a minimum or maximum value of the measure of similarity that satisfies the criterion,

or a range within which or outside which the measure of similarity satisfies the criterion, as

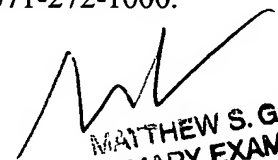taught by Johnson (col. 8, lines 8-12).

Examiner Note

23.   Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the applicant, in preparing responses, to fully consider the reference in its entirety as potentially teaching all of part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter L. Ludwig whose telephone number is 571-270-1365. The examiner can normally be reached on Mon-Fri 7:30-5:00, 1st Fri. Off, 2nd Fri.7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Patrick J. Nolan can be reached on 571-272-0847. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MATTHEW S. GART
PRIMARY EXAMINER
TECHNOLOGY CENTER 3600